BEFORE THE

REGULATORY ENERGY REGULATORY COMMISSION

- - - - - - - - - - - - -x

TECHNICAL CONFERENCE ON: :

CYBER-SECURITY :

- - - - - - - - - - - - -x

Commissioners Meeting Room 2C
Federal Energy Regulatory
Commission
888 First Street, NE
Washington, DC

Friday, December 6, 2002

The above-entitled matter came on for meeting, pursuant to Notice, at 9:40 a.m before the Federal Cyber-Security Panel.

FEDERAL CYBER-SECURITY PANEL:

ALISON SILVERSTEIN, Moderator

LAWRENCE C. HALE
Office of Information Assurance and Critical
Infrastructure Protection, Federal Technology
Service, General Services Administration

THOMAS A. HARPER
Information and Special Technologies Program,
Office of Counterintelligence, U.S. Department
of Energy

LANDIS D. KANNBERG
Pacific Northwest National Laboratory,
Department of Energy

* * *

DANIEL L. LARCAMP, Staff
Federal Energy Regulatory Commission
Office of Markets, Tarriffs and Rates

PRESENTATION PARTICIPANTS:

CHUCK NOBLE
ISO New England, NERC Critical Infrastructure
Protection Advisory Group

KEVIN PERRY
SPP, NERC Critical Infrastructure Protection
Advisory Group

PUBLIC PARTICIPANTS:

LAURENCE W. BROWN
Director, Legal Affairs, Retail Energy
Edison Electric Institute
Washington, DC

LARRY E. BUGH
Manager
East Central Area Reliability Coordination
Agreement ("ECAR")
Canton, OH

MATTHEW CHIRAMAL

Senior Advisor for Digital Technology

United States Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

Washington, DC

LYNN P. CONSTANTINI

Director, Online Services

North American Electric Reliability Council

Princeton, NJ

SCOTT R. MIX

Senior System Analyst

PJM Interconnection

Information Security & Configuration

Control Department

Norristown, PA

STEVEN M. WEBER

Senior Manager

PriceWaterhouseCoopers, LLP

Global Risk Management Solutions

Columbus, OH

JOSEPH M. WEISS, P.E.

Executive Consultant

KEMA Consulting, Inc.

Oakland, CA

CONTENTS

P R O C E E D I N G S

(9:40 A.M.)

REVIEW OF FERC'S SMD CYBER-SECURITY

PROPOSED STANDARD

MS. SILVERSTEIN: Good morning. I am Alison Silverstein, technical advisor to the Chairman at the FERC, and I am pleased to welcome you to today's only -- 14-minutes, starting late -- workshop. The reason we are starting late is so that you could drink your coffee and so that stragglers could straggle in, and since they aren't straggling, we're off.

Let me walk quickly through the agenda, and I will ask the folks sitting with me up at the table to introduce themselves in a minute, but here is the game plan. First off, pieces of relevant paper are over there (indicating) on the side, and I will tell you what they are in case you didn't bring enough paper with you and want some goodies to take home.

The first of the things on the side is the agenda for today. I promise you with so few people, and most of you whom I recognize and we all know what each other is going to say, we can probably rip through this by 12:30 and have a long lunch and everybody catch and early flight or train or something home.

The second thing that is on the table is the original language from the "FERC Standard Market Design Notice of Proposed Rulemaking," and that includes both the text within "Section M" and the "Appendix G" which was the heart of the proposed cyber-security standards.

Then the next piece of paper is the NERC Proposal that was specific modifications that they approved on November 7, and then the fat section is the comments collected from folks, the compilation of comments that people submitted. It includes the entirety of the Canadian Electric Association's comments because they didn't want Stewart really mad at me, and our staff didn't include for some reason skipped the CEA when they were compiling it.

It does not have the appendix of the EEI material for which I apologize, but my staff was in a hurry when they put it together and they didn't realize that they needed to go to the appendix. Yes, Larry, heads will roll later I'm sure.

(Laughter.)

MS. SILVERSTEIN: Those are your relevant pieces of paper. I am sure that you all are so good at your homework that you have already got them all, and they are all highlighted and in your lap, so that is why no one is coming over to the side table, but that is what we've got.

Back to the agenda. Let's go through who is at the head table and why and the reason that -- just to review history very quickly and some housekeeping, the housekeeping is you have something to say you need to come up to one of these and you are going to need to turn on the microphone with the little button and then you will need to turn off the microphone. It is advanced technology, and it works pretty good if we all just keep our faces close to the microphone and our fingers close to the buttons.

The history of this is that in early this year, maybe January or February the chairman, my chairman, met with Dick Clark of the CIPB and Clark said, "Gee, the electric system is very vulnerable to cyber attack."

We said, "Yeah."

He said, "Can't you do something about that?"

We said, "We think so."

This stack of paper in front of you is the result. To do the something about that, FERC, since we don't have a heck of a lot of expertise in cyber-security, turned to the North American Electric Reliability Council's Critical Infrastructure Protection Advisory Group. That collection of industry experts, many of you are members of that I believe or hangers-on, was good enough to prepare a set of recommended standards in a rush and then gave them to us to include as the starting point in the FERC NOPR that went out July 31, and then were good enough to take the rush job and think it through and talk it over more carefully with, again, the participation and assistance of many of you and prepare a set of revisions that are one of these (indicating) pieces of paper that I have been waving around.

The comments that we have received that are compiled in your hands now are on the FERC version that was originally published, which was essentially the NERC CIPAG draft, but our purpose today is to talk not only about formal comments received on that, but also about the revisions that the NERC has proposed through the CIPAG and they have gone through Board review as well at the NERC.

Because FERC has no expertise in cyber-security, except what I have learned from hanging out with you guys and you can judge for yourself how much that may or may not be, I have taken the liberty of calling up some of the folks in the Federal Government who do know what the heck is going on with cyber-security and are in a position to evaluate the sensibility of what you all have proposed within the

NERC and to do a little stretching to make sure that what you all are proposing to us is a good thing.

I just want to take one more minute to go over the context for my Federal colleagues of what it is that we asked the industry to do, and a reminder that what we asked for was minimum daily adult requirements for cyber-security for the electric grid. Most of you have advanced degrees of some kind or another, right, or at least waved at a college driving by and know the course-level system? I think of the kinds of things like "best practices" as at least a graduate level program. Or, if you go to racing, Richard Petty's Advanced Driving School and going on the Indy is probably something like best practices or beyond.

I think of what we asked NERC to give us as more like the learner's permit and driver's ed training. You should know this and you should be doing these kinds of practices before you are allowed to get on the road with the rest of us in order to not only protect yourself, but to protect everyone else on the road. That is the level that we asked for in putting out the cyber-security standards.

Many of you are advocating and working on stuff that goes well beyond that level, and we applaud that and we encourage it and we hope that it will be included in the next generations of the cyber-security standards. I just want to be very clear for my colleagues here that some of the stuff that is in best practices today is not what we think is probably achievable today using immediately available commercial technology at a reasonable cost, at a reasonable implementation schedule on the grid and on grid assets.

Why don't I ask you all, if you would, starting with Tom to let us know who you are and what you do there?

MR. HARPER: I am Tom Harper with the Department of Energy. I am director for information and special technologies in the Office of Counterintelligence. My responsibilities there are to look at the cyber components of counterintelligence and counterterrorism. My history comes from a technology background, information assurance, information protections, information operations. Even though we are counterintelligence and not security, we do a great deal in the monitoring of networks, collection of information, analysis, and we have a great deal of foldover with cyber-security.

MR. KANNBERG: Landis Kannberg from Pacific Northwest National Laboratory. I have about 20 years experience related to energy research. Specifically as applicable to this area, I was providing technical support to the President's Commission on Critical Infrastructure Protection and to the White House Office of Science and Technology Policy in their drafting of R&D requirements for the electric sector. I also led a DoE-sponsored program conducting voluntary primarily cyber assessments in the electric industry primarily at large control centers.

MR. HALE: I am Larry Hale. I am the director of the Federal Computer Incident Response Center at GSA presently, soon to be at the Department of Homeland Security. Prior to joining the FedCIRC, I was at the National Infrastructure Protection Center, "NIPC," for two-plus years where we did a lot of work with NERC and have worked hard to foster a relationship, government to industry.

I applaud Alison's efforts in that, creatively finding a way, recognizing the vulnerability in the electric sector and then finding a way, that FERC can leverage improvements in that vulnerability where in a cyber way you have to creatively find the leverage to do that. I applaud this effort.

MS. SILVERSTEIN: Thank you. Well, our job is to just make other people's good ideas happen. Two of the people who have done the most to make this idea happen have been Kevin Perry and Chuck Noble as the leaders of the NERC CIPAG, and specifically the drafting effort on this. Do you guys want to say anything about yourselves, or did I just steal your lines?

MR. NOBLE: You stole our lines.

MS. SILVERSTEIN: (Laughter) Hey, Jamie. A lot of the people who worked on that drafting are here, so what I will do -- how many of you -- let's see how much of this agenda we can cut out and how much you want to go through for the sake of due process. How many of you, raise your hands if you were on the drafting, on the NERC CIPAG that did this.

(A show of hands.)

MS. SILVERSTEIN: Okay. That is about a third of the audience. How many of you know this stuff cold and have read it and fretted over it and wrote the comments?

(A show of hands.)

MS. SILVERSTEIN: Okay. Larry, you don't count. About half the audience. You do count, Larry, but you are voting twice, and that is now allowed (laughter). About half the audience. You all are observers and you are not cyber-security experts, would that be safe?

(Nodding heads.)

MS. SILVERSTEIN: Yes. Then, why don't we go through an abbreviated version of what is in the security standards. Rather than do two presentations, on the same thing, I am going to ask Chuck to walk us through the NERC revisions that have been propose. Because eventually what they do is they cover the same issues but they fine tune it a little bit, and that way you can explain both what was intended in the original and where you all have some new and improved feature or greater precision.

MR. NOBLE: Okay. Thank you, Alison.

MS. SILVERSTEIN: Can we have the feed from Chuck's computer please now?

PRESENTATION OF NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL'S (NERC'S) RECOMMENDED CYBER-SECURITY STANDARD

MR. NOBLE: Thank you. I will go through this quickly and I will skip -- can everybody hear me?

(Nodding of heads.)

MR. NOBLE: Okay. I will just go through the first couple of slides quickly, briefly. I see that we are bigger than the screen.

(Computer-generated slide presentation in progress.)

MR. NOBLE: For some who may not know, NERC is the "North American Electrical Reliability Council," and it covers all of North America. If you look closely down in the lower left, you see a little jig near San Diego that includes Mexico as well as all of Canada and the United States.

It is made up of 10 regions. To date, that is where the bulk of the membership in the CIP Advisory Group has been drawn from, okay, as well as representation from the Canadian Electric Energy Association, the Edison Electric Institute Security Committee, the American Public Power Association, and the National World Electric Cooperatives Association -- I think I got that one right -- et cetera.

What we are going to be speaking on here this morning, and I will skip through a little bit on the evolution, we will get into basically an overview of NERC's comments, proposals, to what was in the NOPR and why we further commented to what we originally proposed in the first place; okay.

On the evolution, I will skip this because I think everybody knows pretty much how we got to this stage; okay. Does anybody have any questions, want to know any background on how this all came about?

(No verbal response.)

MR. NOBLE: I didn't think so. Very briefly, when FERC came to NERC and the CIP Advisory Group, they basically said what they were looking to accomplish was to establish the minimum daily requirements for cyber-security for the bulk power market and grid operations; okay. That was the task that the CIP Advisory Group picked up on; okay. The intent of CIPAG in doing this was pretty much five-fold. One of the things is -- I can't read my own slide -- I may go through these out of sequence from what you see on the screen.

One of the things was it must be achievable. This must be something that the broad base of electric utilities and market participants, et cetera, could achieve with achieve within the time lines defined by the proposed compliance deadline; okay. This makes it a difficult issue, because depending upon what your role is within the market and within operations, you have an entirely different environment. The kinds of things you might be doing or the way you address doing them could be quite different.

It was very difficult to be really nailing down exactly what we are trying to look for; okay. What we are doing is we are going to be trying to tell people, "This is what you need to do, okay?" It may be more as a policy statement than a standard statement, but you ought to have governance. You ought to have somebody that is in place who is responsible, et cetera. We are trying to define what is the right thing for you to be doing. What we are trying not to tell you right now is how to do it, because that could be different for each individual organization that is represented in this room today.

Your solution to how you achieve that requirement is something I could sit down with each one of you and help you work that out, okay, but I don't think at this time we could put together a program that spells out exactly how each and every one of you ought to do it in one cohesive document.

That is where we are coming from. It must be something that we can achieve, and we must be able to achieve it in a very successful fashion. It must be something that is affordable and cost-effective, okay, meaning that, for example, we are aware that for APPA members, the munies, the "municipal utility companies," they may need time to be able to go back to their constituencies through a very public governmental process to get the funding approved to implement some of these things.

That is going to take them a little more time;

okay. They may not be as readily trained on the technical skills to do this, separate from ongoing awareness training for the workforce in general, but to develop the skill sets within the organization, the know-how, to achieve compliance of those standards may take them some more time simply because we recognize that they are smaller and we recognize that they may not have the funding and the skill sets available in the past. So, they are going to need time to work towards this.

What we are trying to do is establish these as basically the "low-hanging" fruit, things that are so obvious that everybody should be doing that, frankly, I hope you are a little bit embarrassed if you are not already doing it. I think certainly the middle to larger size organizations, the bulk of the requirements they can very readily meet if not today, then very shortly, but it is important that what we present and what we require these people to achieve can be done and can be done successfully within the time lines for compliance.

The bottom line is success needs to be everything in this first step for the industry, and it is just that, a first step. It has been discussed, and it is our understanding, that it is intended for FERC to further regulate not by further regulating specific standards or policy statements in future NOPRs, but simply allowing NERC and maybe NERC and NAESB jointly, as a joint partnership, to evolve additional and more detailed specific cyber-security standards for the industry, that FERC would then regulate by reference to those.

It is truly an opportunity for the industry to self-regulate, and I think it is something that many of us are willing to step up and do. The bottom line is, if we can be successful the first time out the door, I believe success will breed success.

Now a little bit of why NERC has commented to the NOPR when we were the ones who originally provided the draft cyber standards, when FERC came to us in May they basically had barely a two-month time line in which we could draft this and put it together. Anybody who is involved with standards development understands that sometimes standards development can take in large organizations -- certainly in international organizations such as ISO, et cetera, standards bodies -- that it can take up to two years or longer to negotiate and get agreement on what is the appropriate set of standards.

NERC and CIPAG were not able to do all of that even within two months, so what was presented on behalf of this self-corrected work team from CIPAG, the draft went into the NOPR as a draft, not having the opportunity to be fully vetted by CIPAG and NERC membership at large.

However, with the NOPR process and the ample opportunity for it then to be publicly reviewed, that did give NERC and CIPAG participants the opportunity to review it, refine it, decide how we might want to change it. We did that in a couple of meetings in D.C. and down in Dallas. We worked it out, and what came out of that was an approved, across-the-board acceptance that we submitted as our comments to the NOPR. That is where we are today.

The changes that we have done, I am going to focus primarily on providing greater clarity. It is more word smithing, saying it better, not necessarily differently in some cases. We did go back and make some changes specific to better definition of some of the key concepts that we were trying to address.

We did restructure some portions of it where we felt that around compliance, et cetera, that something like that was really more of a FERC issue. It is something that FERC had to decide what that was going to be, not NERC, and it should not be part of the specific cyber standards themselves. We propose that those be moved out to the other body of currently the SMD NOPR.

We did make a recommendation on the time line to (a) the first January 1 time line for 2004 be amended to support a good faith effort to become compliant, recognizing that some entities may be making the effort. They may have made some excellent gains, but just aren't all the way there yet, so we don't want to start penalizing people right away. The first deadline, we would look for that good faith effort, but mandatory full compliance within the definitions of the cyber standards would be required by January 1, 2005.

Briefly, that was what I was just speaking about. Now moving the compliance piece of it into the broader portions of the NOPR, and the issue around application -- "application" meaning who is this applicable to, who must be compliant with the proposed standards -- again, we felt that is an issue that FERC must decide who it is they want these to be applicable to.

That is not an issue that is a concern of the standards themselves. Those are the two things that we really moved out of the standards proposal and are asking that FERC pick up and it is their issue to resolve ultimately what those processes and those definitions will be.

We also recommended that the definition section be removed -- excuse me, adding a definition section. One of the things we had taken out was the references to other standards, guidelines, information, et cetera. Our intent was to designate that we had dealt with other standards bodies, other standards information from NIST, from ISO, the comment criteria, et cetera, as part of our background and quickly try to pull this together, but we have also recognized that in having pulled sort of an amalgamation of all of that, that in a broader sense maybe it was not applicable to make reference to all of those.

We have removed that. We do ask that a specific reference be made to the existing NERC guidelines on security for both physical and cyber, and certainly those would act as more effective tools to help anybody in determining how they would become compliant with the proposed standards themselves.

We also recommend modifying the title of the self-certification form, annual self-certification of compliance with FERC cyber-security standards, that makes it more specific that we are talking about security standards, cyber security and not just security in general. Again, I would recommend modifying certain words and phrasing, et cetera, in "Appendix G" to make it come up and achieve a more clear and concise language.

CIPAG has also provided some additional graphic representation of what we are trying to address with the definition of a cyber-security perimeter. Very quickly I will throw these up. I am not going to speak to these right now. Perhaps, I can bring these up later on when we get to that.

MS. SILVERSTEIN: If you have the summary, these are attached within the summary package in the material, and the summary compilation is arranged alphabetically, so it is about halfway through at the tail end of the NERC comments. For those of you who came in late, we have got all kinds of good paper over here (indicating) on the side table.

MR. NOBLE: Okay. Again, this is another variation to try and give a couple of examples of what we are talking about and how it applies in different business environments within the electric utility industry. There are all kinds of different players with all kinds of business environments, all kinds of physical and cyber environments depending upon generation, transmission, distribution, pure market, et cetera.

Just as the follow on to this, NERC does support the opportunity for the electric sector to be developing its own self-regulation. I think it is a tremendous opportunity. I am not sure how well this has been accomplished in other CIP sectors or in other industries, but, on behalf of NERC and CIPAG, we do look forward to working with FERC and moving forward between NERC and possibly NAESB in developing our own standards.

NERC also supports the goal of all future security standards being developed by NERC in partnership with NAESB. We think that is going to be very much the key process in how this can be accomplished. While they are not here at the table this morning, and I hoped they would be, it was our intention to offer the opportunity to various organizations here, particulary NIST who I think is one organization that maybe has been absent from our process in the past. I certainly would like to extend an opportunity for them to come and attend one of our CIPAG meetings to understand where we are and possibly play an advisory role in future standards development. I think they have a lot to offer.

MS. SILVERSTEIN: I will make sure they hear that. Maybe they had a snow day up north.

MR. NOBLE: Yes. Just briefly, some contacts up there.

MS. SILVERSTEIN: Why don't you, when you get a chance, E-mail me your presentation and we will put it up on our Web page next to the posting for today's conference.

MR. NOBLE: I was still correcting spelling last night. Thank you.

COMMENTS FROM PUBLIC AND PANEL DISCUSSION

MS. SILVERSTEIN: Do any of you have any comments you want to offer right now, just feel free to just hit the button and start talking, if you do.

MR. KANNBERG: Comments and questions

MS. SILVERSTEIN: Anytime.

MR. KANNBERG: Yes. Chuck, the additional year, some of the comments that were provided from the written comments related to an additional year in part because financial budgets had been established for security functions, et cetera, I can appreciate the additional year. Do you need yet an additional year after that in order to get compliance?

MR. NOBLE: Okay. I understand that. Try to keep in mind that everybody knows this is coming and they should be recognizing that there are some good things here, some right things that they ought to be addressing, so they should be already looking at how they are going to do some of this anyway. That would certainly be my desire. That may not be true; okay.

The thing we need to keep in mind is these are not yet the regulated standards requirements, so I think some people are simply waiting to see exactly what falls out so they do know exactly what is they have to address, and also because of budgeting cycles.

I know, for example, the town I come from, Lexington, Massachusetts, our town meeting won't be until March and April and that will set the town budgets starting July 1. If were municipal, that would only give us six months to do what we need to do that we are not already doing to be compliant by January 1, to be fully compliant by January 1, 2004.

With that in mind and considering that these munies are probably the kinds of organizations that don't have somebody like myself or Kevin or some of the people in our audience on staff, they don't have the people then with the skill sets that can pick this up and immediately say, "Okay, this is what we have to do." So, they are going to need some time.

It is not so much the larger and mid- to larger-sized organizations that probably have the staff and funding and concerns about liability and everything else that have been addressing these already and probably don't have far to go, if they are not already there. It is the mid- to small utilities that are trying to be a little more accommodating, so we want them to be successful.

MR. PERRY: If I can add a comment to that also?

(No verbal response.)

MR. PERRY: When the standard first came out, there was a bit of concern about just what these standards applied to and some utilities, some large entities, basically felt in their interpretation that this thing was very, very broad, very widespread, covered the whole gamut and would be very, very costly. Rather than going into their budget planning process with that intention of trying to cover those costs, that is one of the reasons why they would be waiting to find out what the final ruling is going to be.

The timing of the ruling is what is outside of the budget process. The fact that the ruling will not come out most likely until some time in 2003 really dictates, to be reasonable in this, that now that everybody understands what it is they are required to do now they can start planning for it, now they can start looking at where they are compliant and where they have work to do and set up the budgets as necessary to achieve compliance.

We believe, we hope that the entities are substantially compliant already, but we don't have any way of knowing that for sure. We truly do believe that not everybody will be able to be compliant by January 1, 2004, but everybody needs to make a good faith effort to get there. Recognition needs to be made that it can't in all cases be there, and we need to take that in for accommodation purposes.

MR. KANNBERG: A couple of additional questions, if you don't mind, Kevin. The proposal that was provided that standards be pulled basically outside of the document and the intent as stated that the first standards would be sort of the minimum set of requirements and that the expectation is, presumably, a more demanding set of standards would be developed later, is that sort of ratcheting of the standards going to have a dampening effect on people initially responding to meet the first level of requirement because of the concern that future security investments are going to be obviated -- or current investments may be obviated by future requirements?

MR. PERRY: I really don't think so. The

"minimum daily requirements," as Alison has repeatedly referred to these two, are a building first step. I do not believe there is anything in these proposed requirements that would be obviated by future work, except where there is a significant technology change, which you would be well prudent to take advantage of.

You know, if PKI is the standard for today and some great, fantastic new technology for security data communications and encryption and digital signatures, something other than PKI comes out in the future and it becomes a widespread industry standard within the IT industry, then clearly the standards could move to reflect that and there would be a technology change.

In this case, these are all very basic standards. They are things that if you are doing a good business practice today you should already be doing and they are going to be around for a long time, what I see is more refinement and maybe some other areas to look at.

What I would hope, if everybody has been out to the NERC Web site or the electricity sector Web site, you will find that there is something like 13 security guidelines, physical and cyber-security guidelines, and they cover a wide range of things such as protection of sensitive documents. We have one in the works right now for some very basic ways to protect your process control system, something that is not even a part of this discussion.

I would like very much myself, and I think a lot of people within the NERC community feel the same way, that those guidelines should become the basis for standards, but it needs to be done through the NERC/NAESB process. That is a very intensive, time-consuming but thorough process that takes maybe 18 months to two years to work through all of the logistics from inception to an approved standard, but it does get the involvement of everybody. Everybody has a piece of it. Everybody has their opportunity to comment; to refine; and, finally, accept as a standard. In the future, we really do think that is where we need to go. You know, if it becomes a NERC/NAESB standard, it actually has wider applicability than perhaps a FERC-only standard would have. It has a much better acceptance throughout all of the industry -- everybody from very tiny and mini co-op, all the way to the large, half the U.S.-Canada RTO.

MS. SILVERSTEIN: There are mixed feelings about what the goal of this standard should have been. There are many who would like to see, including I think probably you two, in the best of all possible worlds we would like to see a standard that drives technology and that helps to force R&D and force technology to grow to meet the needs that we know exist. Yet from a practical standpoint, to force people to create market pull for stuff that needs to be developed on security to improve the entire suite of technologies that are available out there, and to force people who need to be investing to make those investments.

Realistically, it is not within our power as an agency, nor may it be prudent public policy, to do that. Our goal was much more modest for this. It was merely to try to elevate, reduce the level of vulnerability by elevating everybody's security levels to a manageable degree at a manageable cost using technology and practices that are off-the-shelf today at a reasonable cost, not to impose a huge burden on either the industry or the R&D of the software and hardware sides that feed it.

I do want to point out that when you look carefully at these standards, both at the ones that were published in July and the ones that have come back from NERC in November, you will note that a lot of what is in there is not technology so much as practices. It is not what you spend your money on or whether you are Release 3 or Release 4, but are you badging people properly, are you checking their backgrounds and have you got locks on those doors, rather than merely -- I don't want to say merely -- but rather than on expensive and advanced software and hardware technologies.

We think that these are absolutely no regrets, got to do things. One of the things I am hoping for is that as NERC and NAESB go through developing these things in the future you will be quite aggressive at saying as you are doing the versions, "You need to be putting things out there and making it clear what the technology path for this stuff needs to be. Today, we are doing this. We need that ready in two or three years." That way you are helping to focus the R&D efforts and there is a much greater cooperation and integration to bring some of the needed technologies closer to commercialization faster.

The other thing that is worth noting is that although these standards are written for and by the electric industry, there is absolutely nothing in here, except for the use of electric assets or the electric perimeter kinds of things, that makes them specific to the electric industry. You could remove the word "electric," and put in almost any other sector and these would still apply.

One of the things that, although it is FERC's uncomfortable path to be the leaders in this regard, one of the things I am hoping for is that this kind of approach will get some traction and some recycling in other sectors, so that the electric industry alone doesn't have to bear the burden of developing and implementing these technologies and creating a market for them.

MR. NOBLE: Well, I just want to follow on because your comment about you are hoping that we become more aggressive in developing standards that drive development of better tools, et cetera --

MS. SILVERSTEIN: Just not driving it, but saying we are going to here (indicating) now, and we are looking for those to be ready for Version 3.

MR. NOBLE: Okay. My point was that even if we go to the point where our standards drive what we want to see, vendors start coming back to us with, "Help us achieve it," the fact is that we avoided anything specific to tools or even specific methodologies simply because we are not in the process to start vetting those and doing the certification to make them standard. We really stay away from that certainly at this point in time and certainly in the foreseeable future. We are not ready to go there quite yet.

MR. PERRY: The other thing that is important to understand is there are a lot of initiatives going on right now in parallel with this. NERC has an initiative. We call it the PKI Initiative. It was started by the Electronic Scheduling Collaborative and Oasis Standards Collaborative, and it has got a fancy moniker of "E-Mark." Basically, is a PKI standard.

We are in the process, the CIP Advisory group is now championing this effort, of developing that standard for NERC-wide applications. It has direct applicability to RTO, market systems, et cetera, but it is not done yet, and because it is not ready yet it is not in this recommendation.

There is another activity going on right now actually at the international standards level with the data communications protocol we refer to as ICCP, or "Inter-Control Center Communications Protocol." It is the exchange of real-time data amongst the control areas and the RTOs.

There is a security initiative going on there. It is at the international level. It has reached to the point now where it is, I believe, just about to be submitted for international approval, and it will become a standard of that protocol. Once it becomes a standard of that protocol, then there is a requirement for compliance on the part of all vendors.

Once it is available and then an appropriate period of time for implementation, it can also be incorporated as a requirement under the next generation of security standards applicable in this regard, because ICCP is a protocol potentially that would be used within the critical systems that are covered by this.

The thing to understand here is these standards, these requirements, are very much a living type of document from this point forward. As technologies grow, as new things become available and it becomes something that is just not a quick flash in the pan, but is actually something that has acceptance and would be supported and there would be tools, et cetera, that would be available to support it, that is the appropriate time to then incorporate those requirements as appropriate into the overall standards that would be applicable to the electricity sector, and, as Alison referred to, the other of the critical infrastructure sectors that also wished to adopt these kinds of standards.

MR. HARPER: Looking at this from a different view, it was my privilege to support Landis Kannberg in some of his efforts out looking at the California ISO or the ISM. I certainly understand the breadth of entities that these have to apply to, but I greatly support the standardization, the moving to bringing everyone up to some level. You have a floor defined here.

I think the bar is relatively low, but I think also that it has to be. Other than my personal hobby horse of configuration management, that I think ought to be hit a little harder (laughter), everybody has their own personal feelings, what is the process for FERC to assess whether a good faith effort has been made in 2004 and how we decide if you are fully compliant in 2005?

MS. SILVERSTEIN: That is one of several million dollar questions. If I may stall answering that for a minute, because I don't actually have the answer, I think that is one of the issues people are going to want to discuss.

I made a list, as I was going back through the comments last night, of some of the issues that people were raising. I want to start with a couple of the easy ones and go down to some of the harder ones. That is one of the harder ones.

The easy ones are, What is the technical content? Is everything in here that should be, and are there things that shouldn't be? That includes things like PKI, PCS and SCADA, ICCP, and lots of other stuff that, according to the NERC CIPAG, they didn't think that the particular issues that people wanted to shove in were technologically or commercially ready for primetime yet within the electric industry.

But if people want to have that discussion now, beyond the material that was commented on -- Joe, did you guys file comments? I didn't see any?

(No verbal response.)

MS. SILVERSTEIN: Where did Joe Weiss go?

(Audience indicating.)

MS. SILVERSTEIN: Did you guys file comments on this?

MR. WEISS: On which?

MS. SILVERSTEIN: On the NOPR.

MR. WEISS: That was within the NERC CIP.

MS. SILVERSTEIN: Okay. I was looking for something from KEMA that said, "More on PCS and SCADA," and I didn't see it.

MR. WEISS: I couldn't put it in.

MS. SILVERSTEIN: (Laughter) You were very restrained.

Second, then, there were a couple of details relating to concerns about the implementation of the stuff that is within the confines of this including, for instance, within personnel vetting, are we violating labor laws? How does that complicate things? Issues like that are something that that is why God invented lawyers. It is just beyond my pay grade.

Another equally thorny one, and one also that I will throw to the lawyers, is the issue of protection of the confidentiality of information. I will point out that that seems to have become much less of a problem because the proposed certification form is now so contentless as to be absolutely no issue whatsoever, as far as I can tell. There is not a lot there to protect, as far as I can see, but there may be those in the room who have greater concerns than I or lingering concerns about the protection of confidentiality of this.

There were concerns early on about whether there was an excessive number of physical assets including inside the security perimeter. I am hopeful that the CIPAG's additional work on that cleaned up a lot of those concerns. I didn't see a lot of them within the comments, except some sort of lingering complaints that were not particularly specific. So, I am hoping that one got handled.

There is an interpretation issue that we may not have to handle yet, but at some point we will have to handle. When I say "handle," I mean within the four corners of the document, that at some point we will have to interpret it, and that is what constitutes compliance.

I think Mirant raised this local versus corporate compliance. If you are Mirant, is doing it at one power plant different from doing it at one control room, different from doing it for the entirety of the corporate family of which Mirant is a member?

It has been raised by a couple of different players, and I don't know that we have figured out sort of at what level entities have to file this or apply it. I think that probably will happen in the fullness of time as a test case once these things are out the door.

Application and who must comply, I know that that is going to continue to be an issue. What I am doing is raising all of these so that (a) you know that I read the comments, and (b) you know what is fair games for you guys to stand up and talk about, if you feel so moved.

Self-certification and the due process for compliance, if you don't comply, what are we going to do to you, what are the penalties? All of that is how we use this stuff more so than what is within, again, the four corners of the technical issues, per se, and that is where the real policy issues come down.

People raised the issue within the comments, but there wasn't what I considered to be a lot of really useful clarification of what people's views were. That may be, along with a couple of other things, something that I am hoping we can explore more today and also, if we can stand it, maybe another technical workshop to go over some of the more complex issues here that have policy ramifications and process ramifications now that the CIPAG has done most of the work on the technical issues themselves.

There continues to be the concern voiced by our friends at NRECA and APPA that these ought to be mandatory rather than voluntary, and we sympathize with your positions, but there is that problem of (a) we are FERC and we do standards; and (b) that when you are doing, for instance, air traffic control and you make compliance with air traffic control mandatory for planes over a certain size and let all the little guys do whatever they want to, there are certain risks to the flying public and to the assets incumbent on that strategy.

I think we are sticking with it needs to be mandatory. We appreciate your concerns and we have tried to modify this as much as we can, Barry, within the application section and within the "We're not going to tell you how to do it or what to spend your money on, but here's the stuff that needs to be done." If you feel moved to get up and plead that case some more today, we have got a court reporter and we have got microphones.

Who should monitor compliance and certification? To whom do these pieces of paper get sent? Who is going to verify them? That is another of the heart of this set of issues. If there were only two issues that we were going to talk about today: How do you verify that people have done it, should you verify, and what good is self-certification? If you are Senator Lieberman, for instance, you don't think self-certification is worth a heck of a lot; if you are a taxpayer, you think self-certification is a good thing.

The risk of a couple of violators taking down a system? I don't know what the cost benefit is of that, but I think that would be a particularly useful issue for us to discuss. If you guys want to look as though you made the trip down here on a snowy day worthwhile, that would be one of the topics. Penalties, we didn't really flesh that out as everybody who has read it already knows.

Those were the issues that I saw in reading through the comments and is my sense of what you all continue to be fretting about, and I share your vexation. Some of these have not been handled. We don't know how to answer them. Those are what I hope you all can offer some insight on, and that you all in the audience have some views to share.

That is our script for the comments for the afternoon, and the rest of the morning. If you want to have a nice, meaty discussion of those issues and everybody go off to lunch and we call it a day, that works for me, too. So, I didn't have a script beyond that. Do people want to sort of raise your hands and yell out what topics you want to talk about?

Let's start with what is in the technical content of the first "Appendix G." Did everybody read the NERC response?

(No verbal response.)

MS. SILVERSTEIN: I am looking for some audience participation here; okay. Larry, we know you read it (laughter).

We tried to post this so everybody was on notice that we were talking about the NERC paperwork and the NERC revisions, as well as the FERC original proposal, so my proposal is that we discuss in terms of technical issues. Does anybody have any heartburn over any of the technical issues within the NERC revisions to "Appendix G"? Raise your hand if you want to talk about the technical issues within the NERC "Appendix G."

(No verbal response.)

MS. SILVERSTEIN: I am looking out of the corner of my eye to see if you guys want to talk about anything, too. Do we want to talk about anything that isn't in "Appendix G" that we think ought to be?

(Show of hands.)

MS. SILVERSTEIN: Joe.

MR. WEISS: Nobody else wants to?

MR. SILVERSTEIN: (Laughter.) Anybody else? The fact that no one else wants to doesn't mean that you can't make your pitch, just to get it in the record.

MR. WEISS: All right, then I will.

MS. SILVERSTEIN: Pick a chair, turn on the microphone, and let her rip. Then, just to share with everybody else, Kevin and Chuck will then say, "Your points are superb and here is why PCS didn't make it in."

A PARTICIPANT: Do you just want to say that now?

(Laughter.)

MR. HALE: So noted.

MS. SILVERSTEIN: Not your average technical conference.

MR. WEISS: All right. I am Joe Weiss. I currently work for KEMA Consulting. Previous to that, I was the technical lead at EPRI and the technical lead on cyber-security of control systems. My concern is that the perimeter that has been established does not encompass the control systems that exist within substations and within power plants.

The communication links that have been developed to date as well as the protocols that have been developed to date link these particular systems directly to the control centers. The existing protocols as well as the communications, et cetera, have not included security.

Consequently, what you have is a vehicle for having these systems which are outside the perimeters established by the NERC CIP to be able to essentially penetrate the control center. That is my concern. The second piece to it, and this is just an observation, we have not, and I am using a universal "we," been able to get our vendors, the vendors of the control systems, both SCADA, distributed control systems, et cetera, to recognize that there really is a market to develop secure control systems.

If these control systems would be part of the perimeter and have to be addressed, the vendors would feel that there is a market driver to have to do something. I think if you see here, unless I am wrong, I don't think there are any of these vendors at this meeting, which I also think says an awful lot. Is Alton here?

A PARTICIPANT: Yes.

MR. WEISS: Okay. Like I say, my concern all along is that technology doesn't exist to secure these systems. The procedures needed to secure these systems in many cases are different than IT procedures in that we could establish a significant improvement by simply requiring procedures, address these systems, do it by procedures, make people aware that these systems need to be included, and leave it at that.

MS. SILVERSTEIN: One of the advantages of having federal experts here who work in a bunch of different areas is that I know in addition to the work that the CIPAG is doing on starting on PCS that there are a number of federal initiatives at CHOW (phonetic) and other places. I am wondering if the three of you have any insight?

PCS is a fundamental vulnerability of the electric system, but it is embedded across so many other elements of modern society that I am worried about putting a burden on the electric industry alone to solve what is a fairly ubiquitous problem. I wanted to ask if the three of you know what else is going on sort of at the federal level in R&D? I think Sandia is doing stuff, but I don't know what else is happening.

MR. KANNBERG: Well, I think, as Joe is well aware, NIST and NSA have sponsored a group that is looking at establishment of security for process control systems.

MR. WEISS: I am a part of that.

MR. KANNBERG: Right. I think they are relying on the common criteria approach to help develop approaches and standards. I may be incorrect on that but I think that is --

MR. WEISS: Yes, but it hasn't gone very far. The same point, what Kevin brought up earlier, the IEC Committee, that ICCP is part of, neither that committee nor the PCSRF has been able to this date establish what is called a "protection profile" for either SCADA or

DCS. We don't have that fundamental starting point, even though Jeff Dagle (phonetic) is part of this and Rolf Carlson from Sandia is part of this. I am working with the Idaho National Engineering Lab with the national SCADA test bed. There is work going on, but as the NERC requirements or perimeter has been established that is not necessarily part of it. That is my only concern.

MR. HARPER: Can we hear from Chuck and Kevin as to the reasons it is not included from your perspectives?

MR. NOBLE: Yes. Just very briefly, I will address it from two perspectives, as Scott Mix from PJM takes a seat. Two things, one is, and Joe knows this, that NERC and CIPAG fully share his concerns around PCS and SCADA security, et cetera; okay. The reason it did not make it into the NOPR is because what it really needs is not a one-liner in this document, what it needs is a full-blown, specific standard with a lot of detail focused at those people who have PCS systems.

The second thing is, as Joe was saying, there is not a whole lot out there. The vendors really aren't giving us the tools. I would not want to make a standard statement and hold people compliant to something that is being admitted there is little they can do today. There is little we can offer them or point to as to even suggestions for tools or technologies or methodologies or practices to make PCS or SCADA that much more secure.

I think that is a point that touches a little bit on what Alison said further, or what I interpreted earlier, is that when we do develop these standards and say, "This is what our expectations are," that is what we can take back to the vendors and say, "This is what we want your tools for us to meet. Tell them this is what we want developed." We are just not there yet.

Second to that is NERC and CIPAG is moving in that direction, in parallel to this effort. Kevin, I have asked Scott Mix from PJM, who is chairing a self-directed work team at CIPAG, to address these issues. Scott, if you would talk a few minutes, we would appreciate that.

MR. MIX: Yes. Basically, Chuck said everything I was going to say. My name is Scott Mix, and I am with PJM Interconnection. I agree completely with everything Joe has said. It is a serious issue, it needs to be addressed, and we need to start working on it.

The primary concern that we had in the group, and that I personally share, is one of timing. If we want to have something, and the original intent was to have full compliance by January 2004, we have pulled that back to best effort and do what you can by 2004.

However, the primary driver in that was that the technology and the procedures and the policy and, to a limited extent, standards in other areas exist that you can draw on to do physical security of cyber assets, to do security awareness training, to go out and buy badging systems, to implement all of the other issues that we have talked about. It may take a little bit of money, it may take an amount of time, but it is achievable by everybody in the timeframe that we have laid out.

What we don't have is the technology available to implement what we really consider to be the required security in that what was initially 12 to 15 months and is now pulled out probably 18 to 24 months from the time that the rule is issued. I think that is the primary, or is going to be the primary, driver behind the next evolution of these standards. The Version 2 of these standards needs to start addressing process control systems and communications protocols that Joe has talked about.

As was alluded to, I am heading up the NERC CIPAG effort in doing process control system security.

I am working with Joe and all of the people Joe has mentioned. We are trying to engage the vendors, we are trying to engage the end-users, we are engaging the consultants, and we are engaging the industry experts. Anybody who wants to have a seat at the table we are welcoming them, and we value your input.

We need to get that problem solved, but it is going to take more than 12 to 18 to 24 months before we can get something that is going to have mandatory compliance both developed as well as implemented by all of private industry.

MR. KANNBERG: I certainly appreciate and would endorse the concerns particularly about high-level SCADA systems and EMS and the communications protocols and systems associated with those.

Getting back to Joe's point, I have become a little concerned about how you define the boundary of the perimeter once you cross the plant boundary and you start including the process control system at the plant. Many of those systems are interconnected back into corporate networks, so I think that becomes very fuzzy as to where you draw that boundary.

I think the effort focused on defining that boundary in a way that allows you to, in fact, implement adequate security measures. Because the larger the perimeter of your system for security measures, the more difficult, the more costly, the more complex it is to implement security, and in most cases it becomes not only more difficult, but you increase your vulnerabilities when you expand your system. So, I am sensitive to the fact of drawing the boundary at a level that you can reasonably administer security.

MR. PERRY: I would like to make a couple more comments germane to this. One, I fully support what Dr. Kannberg mentioned about the larger the perimeter -- I mean, it is not a linear cost factor there at all. What the CIP Advisory Group focused on with these set of requirements was guidance given to us of protecting the wholesale electric market and protecting the reliability of the high-voltage transmission system to the point that an attack, a successful compromise, would not result in the collapse of the wholesale market, would not result in a widespread blackout due to loss of transmission reliability.

That there gives us a good limiter of what we need to focus on. From the very beginning what we have said and what FERC has repeatedly told the CIP Advisory Group is to focus on the critical assets that have a high impact. Really, security is an issue of risk management. You have got so many dollars to apply, and you need to apply them prudently.

If you take a look at the electric systems today -- and before I came to Southwest Power Pool, I worked for a number of years at Entergy, a rather small electric utility that nobody has ever heard of -- there is an awful lot of stuff out in the field that is about as old as I am. It is not something that is going to be cost-effective to go out and do a wholesale replacement of the entire infrastructure to add a modicum of security.

There certainly are steps that can be taken from this point forward. There is new technology coming in today. They are beginning to use the Internet, which I have my own opinions on, but they are not appropriate to say in public with Alison and women present in the audience.

MS. SILVERSTEIN: It is the court reporter's ears you have to worry about.

(Laughter.)

MR. PERRY: (Laughter) Yes. Certainly, use of certain operating systems that get a lot of play today, where they are not secured real-time systems, one particular operating system you read on the box and it says very specifically "not for use in critical applications" and yet they are building EMS systems with it today, I have some concerns about that. That is where, part of where, we need to be focusing our efforts on getting the vendors to change their philosophy.

The problem with that is you have got the customers out there that want absolute, rock-bottom dollar price. They want to buy that Volkswagen and they want to feel that they are buying a Lincoln Continental, okay, but they only want to pay the Volkswagen price and they want to get a used Volkswagen while they are at it.

We have an issue of cost; we have an issue of retrofitting. One of the things that the PCS Working Group is working with the vendors in the Self-Directed Working Team is looking at is there some sort of relatively effective, relatively inexpensive way of retrofitting something, maybe putting something in line with the communications circuits to do security.

We are looking at some of the very basic vulnerabilities that you have with a process control system. One was mentioned, connectivity to corporate networks. Just common sense good practice says that if you have connectivity to your corporate network, you define the perimeter around your critical system and you firewall it and you put in your IDS and you do what you need to do to protect it.

The fact that it sits in a generation station out in the middle of nowhere versus your expansive control center is immaterial. It is common sense to do that. But you then weigh that, for the purposes of these requirements you have to weigh that, against if somebody attacks the process control system at the Cherokee Power Plant, what is the impact going to be on the electricity sector? The fact of the matter is probably not a whole lot.

Do you go out and mandate vast amounts of expenditures and mandate them under the FERC standard, or do you work with the industry and do the awareness, do the risk management, do the risk assessment and get industry to recognize that they need to take very basic steps and just because it is not in this particular standard, which is applicable to the wholesale market, doesn't mean that it absolves you of the responsibility?

The insurance companies charge you based on the risk assessment. If you have very good best practices, the insurance companies will reward you by reducing your insurance premiums. Your lawsuits will be far less if you have good risk practice and show that you are not grossly negligent and you did a best effort to protect yourself. That is something that any business has an obligation to do without us having to sit up here and demand you to finally wake up and do it.

You know, the focus that I think these requirements need to be on is the large impact -- the focus of the reliability of the grid; the focus of the protection of the wholesale market, which really is where FERC has jurisdiction, especially in the wholesale market -- define the critical assets with respect to that, and then the awareness is the other part of it.

MS. SILVERSTEIN: Let me ask the four of you, all of you, are there measures within the recommended security measures that we have in place within "Appendix G" that help to mitigate or limit some of the potential damage that a PCS failure could cause?

MR. PERRY: I will address that first, if I may. The answer is yes, I believe so. Because the original "Appendix G" had a separate section that we actually put in to address issues with PCS. When we went back and revisited, we looked at it, we were saying the same thing. Rather than just repeating ourselves, it does make sense to turn your modems off, put in your electronic access control points like your firewalls.

I mean, like I just said a minute ago, it doesn't care where that system is. It can be in the plant. If it has got connectivity to the outside world, it needs to be protected. The stuff that is in "Appendix G," the enumerated things that you need to do to protect, are very much applicable in many cases to the process control system.

Yes, I think it is applicable without specifically calling out that we are talking specifically about a PCS, without including it specifically in the diagram of the covered perimeter.

MR. HARPER: If I may be so bold to propose a suggestion, it is very clear you are trying to focus on the biggest impact, the "low-hanging fruit," as it was called earlier today. Also, everyone agrees that this is a very serious issue, and it is going to be addressed in the future. One of your stated aims is to get the attention of industry, both the electric industry and the SCADA PCS type industry, to be aware that we are going to have to start addressing this.

Would you consider putting into your documentation a statement of future intentions? Because I feel if you are going to be changing the definition of your security boundary, if I was on the receiving end of these regulations, I would like to know if they might change over the next two to five years. If I am having to do my budgetary planning several years out, I would like as much advanced warning. That may be a vehicle, since you are already moving in the direction to bring these together, just to put everyone on notice that this is coming.

MS. SILVERSTEIN: A good idea. Thank you.

Larry?

MR. HALE: Not being a lawyer and not having played one on TV, I would also like to suggest that we may want to have some wording in there to clearly state -- recognizing the perimeter as defined in this document does not include those remotely located PCS components, but acknowledging that some of the steps and some of the recommendations would help security of those systems and clearly stating it, I think, to protect the drafters of this and the supporters of this document from basically being liable for, "Well, nobody required us to secure those things" -- why that is outside the perimeter and including that statement of future intent. Again, you would need to have the legal beagles address the wording, but I believe that is necessary.

MS. SILVERSTEIN: That is a good idea. My only concern about adding a statement of intent is that it will require an extra page of legal disclaimers to go to the effect of, if we say we want to go in this direction and look at these, and then three years down the road, when we either don't address all of them or add additional things, we will end up with great quantities of whining about, "Why didn't you do this? Why did you do this when you didn't warn us?" But that is what lawyers are for. They are both good ideas, so we will see what we can do to legal them over.

MR. PERRY: Just a consideration, the ultimate goal I would hope is to turn this over to the NERC/NAESB process for the proper development of standards using the proper bodies, the CIP Advisory Group being one. We do have work going on in this area already. We have the security guidelines that very likely should and will be codified as standards. I would think that actually is the proper venue to do that.

I think in the end there needs to be more than one standard. One standard, "one size fits all," just doesn't do it. I think there needs to be a security requirement developed specifically to PCS. The Self-Directed Working Team that Scott Mix is leading is the proper group to initiate that within the

CIP Advisory Group context, and we are already working on that. Hence, the security guideline that we have already developed that will be up for approval by the advisory group in January and upon approval will be posted out on the Web site.

I would really, rather than trying to incorporate something into language of the FERC standard, I would like as an alternative to maybe make comment of the fact that the standards will continue to be developed, but it would be preferred to be developed under the already in place industry process, which gives us the fairness, openness, balance and inclusion that several of the commenters did respond to in the document. Let's work it that way rather than trying to come up, "Well, this is what we intend to do in three years, five years," and get into all of those legal rangles (sic).

MS. SILVERSTEIN: The PCS issue along with the information, confidentiality and protection issue both highlight something that we are all painfully aware of at this table, which is the fact that this is not a set of issues which is unique to the electric industry. It would be a great relief if the new Department of Homeland Security could put together some legislation that addresses many of these broad-reaching commercial and industrial problems across the board.

I mean, the reason that we are having this discussion today specific to the electric industry is because we are grappling with it, but similar discussions are occurring in many other industries in separate venues wrestling with the same problems. We really need some more effective tools and some more effective cross-cutting addresses and efforts to deal with it.

I think we are hampered by the lack of -- not a lack of federal effort, because I know how much you all are working on this and your colleagues out in the labs and elsewhere -- just the lack of federal "umph" in terms of legislative authority behind it. So, we will just put that in as a marker.

Thank you for the PCS discussion. Did you find that helpful at all, Joe?

MR. WEISS: The concern I had really was simply the fact that when you read, if you will, the introduction, it appears as if this is only applicable to, if you will, the control center people, which is traditionally what FERC and NERC are involved with.

Like I say, my concern is I just wanted the others, if you will, at the substation and plants to understand this also impacts them. It isn't necessarily that I want to necessarily move the perimeter, but so they realize this also has an impact on them. As it is written, I am concerned that they won't feel this has any impact. That is all I have to say.

MS. SILVERSTEIN: Got it. Thanks very much.

MR. WEISS: Thank you.

MR. KANNBERG: Can I reflect on that just a little bit more, Joe?

(Nodding head.)

MR. KANNBERG: I appreciate that. Is there some distinction of certain plants that might be included as critical assets, must-run plants, things of this nature that would allow some sort of descritization of the --

MR. WEISS: No. I will tell you where I am coming from. It has nothing to do with the individual plant, and that is where Kevin and Chuck and I have talked before, it has to do with the fact that each plant that uses protocols that go directly into the control center could potentially compromise the control center.

It has nothing to do with an individual plant. You know, where Kevin said Cherokee, it has nothing to do with that. It has to do with here is a potential vulnerability into this bigger area. That is why I don't want to focus on any specific, because we can tolerate loss of power plants and loss of substations. It is the compromise of the control center I am concerned about. Does that help?

MR. KANNBERG: (Nodding head.)

MR. MIX: If you look at the way the perimeter is currently drawn, it does indicate on the drawing that there are interfaces out to field devices and alternate control centers, and we carefully drew that red dotted line so that it bisects the communications equipment that interfaces to those outside plants or external field devices.

One of the reasons we did that was because we needed to implement some kind of a policy device. We refer to it as "firewall," but it could be a commercial firewall; it could be a gateway device; it could be a communications front-end processor with line buffer cards on it; or it could be a router with some access lists, some very primitive firewall devices or firewall rules.

We wanted to draw the line to attempt to contain when possible any kind of a security breach so that if a plant, a specific plant, or substation had an incident that that incident would not automatically gain it access into the larger control system in the market systems.

As I said before, we wanted to do something that was easily attainable in the timeframe, but we clearly recognize that we need to expand that security perimeter to include other devices and other technologies, but we need to do it in a timeframe where there is a technology that we can actually implement somewhere.

MS. SILVERSTEIN: Let me change the subject, if I may. Kevin, do you really have to say it, or are you just leaping for the mike button?

MR. PERRY: The quick comment I was going to make is that depending on the protocol between the process control system and the control center, that will determine what the appropriate what the appropriate protective measure is that needs to be taken at the control center. That is where that protective perimeter is.

If you are coming in over a wide area network, you have very clear protocols, very clear protections; if you are coming in over a dial-up using arcane bit protocol that is not really exploitable, you have a different degree of protection necessary. That is why the perimeter is drawn at the control center. We are protecting the control center from everything outside, and we need to do that effectively.

MS. SILVERSTEIN: I just want the few FERC people who are monitoring this to know that every time I go to a CIPAG meeting I listen to two days of this, and I want to start getting combat pay.

(Laughter.)

MS. SILVERSTEIN: It is making me a much better woman, though. Let me ask, I think, rather than -- does anybody else have any specific issues about the technical contents of what is or isn't in "Appendix G" as revised by the NERC?

(No verbal response.)

MS. SILVERSTEIN: Nobody has anything; okay. Let me ask the further question of, How many of you are sitting in the audience because you feel paranoid if FERC does something that you are not paying attention to--? Raise your hand.

(A show of hands.)

MS. SILVERSTEIN: Okay. And, how many of you are sitting here because you have something burning to say about something that is specific to -- I mean, when I say you have something to say, that means you are sufficiently motivated to get up and sit at one of these microphones and talk on behalf of your client about one of these issues?

(A show of hands.)

MS. SILVERSTEIN: Okay, this is where -- Joe, thank you. Because otherwise it is going to be a really short workshop; okay. Also, we have got Larry, who also wants to say something. If nobody else wants to talk, I will just tell everybody the story about the natural gas -- okay, this (indicating) gentleman -- workshop we were at yesterday, which was a pleasure for students of irony everywhere (laughter). It has embarrassing moments for NERC in it. We will save that for the wrap-up.

Why don't we get Larry's comments and this (indicating) gentleman's comments. If you all want to, come on down. Then, why don't we indulge in a few minutes discussion -- hey, Dan -- of if you all want to about the compliance and the verification and certification issues, and then we will declare victory.

Larry?

MR. BROWN: The red light is on, yes. Larry Brown with the Edison Electric Institute, representing investor-owned electric utilities. This really has to do with the more policy issues. I appreciate what Alison had said earlier about what the CIPAG proposed was technical issues, and what was pulled out was anything that even smelled a little bit like a policy issue.

Now we are at a stage where we can talk here today a little bit more about the policy issues, and I only want to stress that it is extremely important that FERC make very clear who it is they expect to be subject to security requirements as well as any other of the requirements of the SMD NOPR. Who is it that are market players? How do you determine a market participant? Is it every marketer who is running a computer out of their garage, or just the big guys? Where do you draw the line in between?

I also think -- and in particular this relates to these technical standards, in general to the issue of ongoing standards development in the industry -- that it is necessary for a certain degree of specificity about who is going to take care of what area of issue and what do you do if, as today, we have two bodies generally focused one on reliability, NERC, and one generally focused on business, which is NAESB.

If that is going to continue, then to get some guidance as well as encouragement from the Commission as to the expected role that each will play and the expected interface that they will have where these roles overlap and cannot be pulled apart, which I think really the security issue involves, it is clearly an appropriate role for NERC; it is clearly a reliability issue. However, it obviously has business implications, and, therefore, I think it is also clearly a role for NAESB.

I personally, and I think on behalf of my industry, would appreciate a great deal of both specificity as to what FERC expects, but also encouragement for a particular kind of process so that we have confidence as we move forward that it is going to remain appropriate for both NERC and NAESB, or whatever it is that you come up with, to continue playing in this field.

Again, as an advocate, I think it would be a shame to throw away what has already been done at NERC, but I think it is also very necessary to encourage the NAESB folks to become more involved than they have been, and to also encourage the development of a formal rather than an informal process for working together. Informal processes sometimes have a habit of falling apart.

MR. LARCAMP: I am Dan Larcamp from FERC staff. I have read it only once, but doesn't the NERC/NAESB MOU that has recently been signed move a long way in that direction by basically documenting the procedures the two agencies will be using to sort of make sure that something that starts out looking as reliability gets the business input and vice versa, as well as, I think, expressing on behalf of both organizations sort of a philosophy that we are going to cooperate rather than confront in working through these issues?

I guess I have heard that document will be filed with the Commission. I guess I am wondering what further specificity, beyond the procedures that are set forth in the MOU, would you be looking for? I guess we will see that if comments come in.

MR. BROWN: Actually, it is good to hear that you are aware of the MOU. I am very happy with that. It reflects a great deal of work and a great deal of commitment on behalf of both organizations. You know, again, as an outsider I don't represent either one. That the Commission appears to be, based on your comments, willing to accept that MOU once it is filed, or perhaps suggesting that it should be filed rather than merely expecting that it will be filed, those are the kinds of things the Commission could do -- recognize and accept and move forward. Those sorts of statements would be very useful.

Obviously, we are in a transition period. We know that there is an MOU. It hasn't been filed, so forth and so on. Those are the kinds of issues that I am concerned about, and it is good to hear back from you, Dan, that you are really moving along the direction that I was proposing.

MS. SILVERSTEIN: As you know, everything in this industry appears to be in a transition period. My personal view is that the MOU doesn't go far enough. In fact, there needs to be not just an MOU between NERC and NAESB, but there needs to be a very explicit recognition and divvying of responsibilities between NERC, NAESB and the RTOs/ISOs because each of those organizations or types of entities have different skill sets and competencies as well as responsibilities.

The MOU talks nicely about processes, but doesn't actually get down and dirty about, "Here is an issue. Which side of the fence does it fall on?" I think more needs to be done in the way of these three groups and interests working and playing well together in carving up the turf in a constructive way, that prevents future squabbling and helps make some of the decisions and processes cleaner in the future. That takes us into the software standardization, which we won't cover in this particular workshop.

Sir, did you have something you wanted to talk about?

Thanks, Larry.

Please tell us your name and organization?

MR. CHIRAMAL: My name is Matthew Chiramal. I am with the Nuclear Regulatory Commission, and I just wanted to bring you up to date as to what we are doing and to make sure that we are consistent with what your regulations are going to be like.

As you know, being very sensitive about cyber threats, we had to do something very initially and we imposed some interim measures regarding both information systems and control systems to be looked at to make sure that some of the vulnerabilities that we identified are taken care of.

At this point, we are working with the nuclear industry. With the help of Landis' people, we are going to review four nuclear plants and come up with a methodology for all of the plants to look at the vulnerabilities of the systems. We would like to be consistent with the requirements that you are imposing at this point to make sure that we are not going out of the way.

We are also waiting for the Department of Homeland Security to come in with what we call the "design-basis threat." What is the insider threat?

What is the outsider threat? What combination are we looking for? We are looking for interconnections such as even what we call "virtual connections," that means some software written outside coming into the plant through the floppy or a CD which should be considered, access control and things like that. I just wanted to make sure that we are consistent.

MS. SILVERSTEIN: Thank you very much. We have been following what you all are doing. It is our impression and fond hope that what is in -- and if you feel otherwise, please tell me -- "Appendix G" is well below anything that a nuclear plant would be doing in terms of protection of its own assets. We were hoping that you all were in fact, to go back to my earlier analogy, if this is driver's ed, we are hoping that you all are in graduate school and beyond (laughter) in terms of nuclear assets cyber protection. Is that correct?

MR. CHIRAMAL: Yes, that is correct.

MS. SILVERSTEIN: Thank you. Yes, I am pretty confident we are not getting in your way.

MR. CHIRAMAL: We work with CIPAG. In fact, we are members of that CIPAG, so we are working, trying to make it consistent.

MS. SILVERSTEIN: Thank you so much. Let's see, sir, if you could give a copy of your business card to this lady (indicating), we would appreciate it very much.

MS. SILVERSTEIN: If anyone else has anything they want to talk about? Others on specifics?

(No verbal response.)

MS. SILVERSTEIN: Why don't we move, then, to see if anybody wants to talk about compliance and verification. Is there anyone in the audience who wants to talk about that? Are we going to chat amongst ourselves? Are we done?

Kevin?

MR. PERRY: I will kind of lead off here. I want to characterize this as my personal opinion. I have not polled the CIP Advisory Group in the form of a motion to have this endorsement, so it is purely my opinion. My opinion is that once the standards, assuming that it happens, once they are shifted to the NERC/NAESB process, that NERC has a compliance program.

It has a penalty assessment capability built into it, even though NERC today, with the exception of voluntary participation in a couple of NERC standards, it is a paper exercise right now. There are not nasty letters sent to public utility commissions, there are not fines levied, et cetera.

However, there is a structure in place through the NERC Compliance Program complete with field audits every couple of years, self-certification on the interim years that would make an excellent vehicle, I believe, to deal with the compliance part of the requirements for security.

With the field audit, it goes a little bit beyond the self-certification. Every three years somebody sits and takes a look at your books, and you have to demonstrate more than a piece of paper with a signature on it, but that you are, in fact, cognizant of the requirements and you are doing a good effort to comply.

It has a graduated penalty factor for non-compliance, depending on how badly you are out of compliance, with how many requirements you are out of compliance, how many consecutive times you have been out of compliance. It gets consecutively more painful to you to where you are finally incented (sic) to fix the problem because it will be cheaper than continuing down the path of non-compliance.

I would offer to the Commission two things: One is to very strongly consider pushing the standards development and compliance into the NERC process, working with NERC to develop that. I am not speaking for NERC either, so NERC has got to nod their head and say, "Yes, this is a good idea."

MS. SILVERSTEIN: They did that already.

MR. PERRY: If that is not done, then I would ask that the Commission take a look at the NERC Compliance Program, the penalty piece of it as documented, and consider using that as a basis for any compliance penalty phase that FERC would impose on any entity that is subject to these standards.

MS. SILVERSTEIN: The revised NERC recommendation says essentially start compliance effective January 1, 2005; right? Four or five?

MR. PERRY: Substantial compliance, 2004; full compliance, 2005, yes.

MS. SILVERSTEIN: Right. Essentially, 2004 is advisory and 2005 is mandatory?

MR. PERRY: Yes.

MS. SILVERSTEIN: It would be probably the earliest that there would be NERC's process in place. What would be the earliest? That is question one. Question two is remind me pay for NERC.

MR. PERRY: Well, I am not sure I am qualified to answer all of those questions. NERC does have a compliance program. They have compliance managers at NERC Headquarters, and they have compliance managers at each of the regions. It is an active program they develop on an annual basis. In fact, I believe they may be meeting this week -- this week or next week to develop next year's program. It is a somewhat contentious program in some areas as they work out what the actual standards are and what they are going to do compliance on this particular year, but it has been a growing process.

There has been only a handful of standards that when they did the compliance test, if you will, and they found that the compliance standard may be needed to be reworked or something, they pulled it out of the program or they went back and reworked the standard. However, they add, more often than they subtract, standards to the compliance every year.

The electric entities, the control areas, and I have knowledge of Southwest Power Pool, I don't have knowledge of any of the other regions, but within the Southwest Power Pool we have seen significant progress on the part of our members to achieving full compliance with the Compliance Program.

So, I think it is an effective program that can certainly be done. How long it would take to incorporate the security standards into that program? I don't know. I am not part of the Compliance Program group, so I can't answer that.

MS. SILVERSTEIN: Essentially, we are looking at, if the standards were adopted next spring we are essentially looking at, more than a year and a half before there would have to be something in place to start with, a compliance process. Is that the kind of thing NERC could ramp up? I am hesitant to -- this Commission, to be perfectly frank, is not in the business of doing field audits of cyber-security. I hope to God we never are.

It seems to me that I would just as soon get people used to whatever the process is. Figure out a smart process from the beginning and get it in place and get it ramped up over time as the standards ramp up, as the compliance process begins, rather than having some ineffective interim in place and then having it transition and having NERC go through a practice ramp up itself.

I would rather just get it right from the start. If NERC is the place where it is going to end up, let us build that capability faster and have it in place when it is time for the compliance program to start rather than to do some transition. That is me personally talking rather than this Commission.

Anyone else? You clearly have views about compliance, so jump in.

Tom?

MR. HARPER: Where is the boundary between the NERC compliance and FERC's authority? Because it won't be NERC meting out the penalty, it would be FERC that managed that. That is the biggest gray area that I see. I don't see a natural mapping there.

MR. PERRY: The issue as I understand it -- and once again I want to reiterate that I am not a NERC employee, I am not part of the Compliance Working Group and I don't have any direct responsibility for the Compliance Program -- my understanding is the process is the first step is going to be the enabling legislation that turns NERC into NAERO and basically gives it the self-regulation piece with, I guess, FERC oversight or whatever the oversight is that is into that legislation. I am not a hundred percent up to date on it.

Prior to that, there really isn't any "teeth," unless the NERC membership volunteers to accept the penalties, which they have been working on for a couple of standards, disturbance-related type standards. So, prior to NERC being in a position to actually enforce with sanctionable penalties the standards, it would have to have a little help from some entity that can.

Once the enabling legislation is in place, then I believe that NERC would have the ability to enforce the sanctionable penalties.

The problem is I can't predict. My crystal ball is shattered in so many pieces on the floor right now, you know, I don't even cut my feet stepping on it anymore. I have no idea when the legislation will eventually get passed. You know, we keep working on it every year, and every year it gets postponed for yet another year. It is a question I cannot answer.

Could NERC put together a program that at least went through the effort of doing the assessment, doing the self-certification? Once again, I am not able to speak for NERC. My personal belief is that if that challenge was put before them and NERC accepted it, the compliance managers accepted that, yes, they could.

The standard requirement will be in front of them, and it is simply a matter of identifying the qualifying questionnaire, identifying the items that need to be looked at when they do an on-site assessment, and developing the compliance program around that standard. I would think that they would be able to do that; but, once again, not being a part of that particular effort, I really don't want to speak for them.

MS. SILVERSTEIN: By talking about NERC and its compliance field audits program, you take me to the next question which is, What is the role of self-certification? What is the value of self-certification? Do you, to quote a past president, "trust but verify"? You are clearly in the "trust but verify" school, I submit.

Is there anyone in the room who thinks that self-certification is sufficient and there should not be some sort of auditing or compliance verification program? If there are any advocates of "No we don't care how important it is, leave us alone. If I tell you it's legit, it's legit"? Is there anyone who wants to advocate that point of view? Or, is everybody here comfortable with, "Okay, bring on the field audits"?

(A show of a hand.)

MS. SILVERSTEIN: A brave man.

(Laughter.)

MR. BUGH: Larry Bugh from ECAR. Alison, even the NERC Compliance Program has self-certification with periodic on-site visitations and assessments, so I think that the self-certification is still a valid thing. I think it is something that we would have to take another look at the self-certification form that we have today, and perhaps go back in, in the case of the existing NERC Compliance Program, for which the self-certification form is much more detailed than what we have in the SMD NOPR for cyber-security.

It would have to be something, I think, that would be much more detailed. It would be more specific as to the things that an entity is self-certifying themselves for, and then it is something that an audit team can come back on a periodic basis, follow up on to check and make sure that what they are being given as a self-certification is truly the "state of the union," if you will, in that entity.

However, I think that there is a place for self-certification. You are not going to have enough folks to be able to do an on-site, honest to goodness audit of every entity every year in order to make sure that folks are staying in line.

MS. SILVERSTEIN: I agree with you. I think the distinction is not -- yes, self-certification is the first step. However, the question is, Is there a second step with respect to compliance? I hear you saying yes, I think. The question is more, How detailed? The question after that is, What happens if you don't comply? As long as you have got a microphone, go for that.

Larry, come on up.

MR. BUGH: I think that is right. There is a two-step process. I think that the self-certification is something that needs to be done, but, again, I think it needs to be in more detail. Again, there were comments on and one of the recent self-certification form that was in the original draft got pulled was because there are a lot of questions about, "Who would that go to? Who would that form go to? How is it protected? How is the information protected?" those kinds of questions.

Those certainly all need to be worked out before any kind of a detailed self-certification form could be developed. However, I believe in the long-term, if NERC is going to be the entity that does the compliance monitoring of the standards, then I believe that a self-certification format is the appropriate way to go with follow-on visits on a periodic basis.

MS. SILVERSTEIN: Larry, go on.

MR. BROWN: Actually, he kind of made my point. If FERC is going to get self-certification forms, we have a concern about the privacy of the information submitted. If NERC is going to receive self-certification forms, it is much easier to deal with because we can have non-disclosure agreements with

NERC. There are lots of ways to protect that information, and then obviously there would be a reasonable point to having a more detailed form.

Just to reiterate what Larry did say is that our concern, which lead to making the FERC form much less detailed, was simply that we did not want to put ourselves in the position of having to worry about what we were telling the public at large by virtue of filing a form with an agency that may or may not be able to keep it out of the public hands, depending on how FOIA is interpreted by some court ruling down the road or how the Critical Energy Infrastructure Information Rulemaking turns out and then is interpreted by a court ruling down the road. We just avoided that and made a very simple form. If NERC is going to do the audit as opposed to FERC, then NERC probably has a need to get more detail.

MS. SILVERSTEIN: Let me go down a side road for a second. The original proposal was to send this stuff into FERC. You all changed that in "G" in your revisions and said send it to us or to NERC? Remind me.

MR. PERRY: We said send the certification statement to FERC. What we removed was the detail of, "This is what I am and I am not in--."

"If you are not in compliance, call your friendly FERC point of contact and let's have a little dialogue here."

MS. SILVERSTEIN: Okay. There were some commenters who said don't send it to FERC send it to your RTO, ITP, ISO, fill in the initials of your choice? But now what I am hearing is stick this all on NERC and get FERC on it, and get the ISOs, RTOs, ITPs out of the business entirely?

MR. MIX: (Nodding head.)

MS. SILVERSTEIN: Scott is nodding. Does anyone else want to nod on that?

MS. CONSTANTINI: (Nodding head.)

MS. SILVERSTEIN: Okay. Jamie is nodding.

(Laughter.)

MS. CONSTANTINI: Is this the time I need to say something? We are being drafted, I think.

(Laughter.)

MS. SILVERSTEIN: Before I forget, if you all could also give your business cards to this lady, we would appreciate it a great deal, before you leave.

MS. CONSTANTINI: Sure. I am Lynn Constantini, a member of the NERC staff. I do feel compelled at this point to join the discussion. Yes, we do have a compliance program. The director of that compliance program is David Hilt*. Currently, they are assessing compliance to planning standards and operating standards strictly in the reliability arena. I do not know if David has considered security standards including them in his compliance program.

I agree with you, Kevin, that we don't have the "teeth" right now. The compliance program has been very successful. Even as a voluntary program, it has been very successful. With the passage of the legislation, I believe it can be even more so. I do believe that security standards in that they do affect reliability would be a natural fit. What I would like to do at this point is to extend the invitation to you, Alison, to have a conversation with Mr. Hilt on the subject and pursue the cooperation at this point.

MS. SILVERSTEIN: I would be happy to, and I think the phrase "job security" will come up.

(Laughter.)

MS. CONSTANTINI: Thank you.

MR. LARCAMP: When you say "NERC," you are talking Princeton rather than Regional Reliability Councils? I mean, some of the reliability stuff in the Midwest was handled by an area -- I am just trying to understand. Because there have been a couple of instances when NERC reliability rules were not followed and filings were made by Reliability Councils to, in effect, have penalty authority put on file with the Commission, the WECC, WSEC then, on the loop flow and the ECAR problem.

So, I am just trying to make sure that from an affiliate perspective that I understand who is going to be doing the monitoring. If it is ECAR monitoring ECAR, then, gee, maybe I have got a little concerned there. If it is Princeton monitoring participants in ECAR, I am less concerned.

MS. CONSTANTINI: Not being a member of the Compliance staff, I really don't know what the rules and responsibilities are, but I think when you engage in a conversation with David Hilt, he will clarify those points specifically for you.

MS. SILVERSTEIN: Larry?

MR. BUGH: As far as the Compliance Program is concerned, it is a program that is established by NERC, but the Regional Reliability Councils, just due to the size of the organization, do play a significant part in enforcing and implementing the Compliance Program.

So, when we are talking about would it be an ECAR entity that is assessing and ECAR member company, yes, we have a compliance manager on staff at ECAR who goes out today and who collects the self-assessment forms, who goes out and actually does the on-site audits, who in a trial program -- we have two programs within ECAR right now, we have a contractual and a non-contractual.

If you are someone who has signed on to the non-contractual program, then what you end up with is phantom penalties. If you are out of compliance, there are letters to go to your CEO and things like that, and there are copies to go to NERC for filing with NERC staff so that they know that we are doing the job at the regional level.

If you are part of the ECAR contractual program, then I believe it is next year there will actually be honest to God financial penalties if you are out of compliance. As we move forward, hopefully with the implementation of the legislation to make NERC into NAERO, then that all can be formalized across the board.

But, yes, there will be ECAR folks doing assessments of ECAR member companies. Now, if we are talking about an assessment of something at the ECAR office, are we in compliance with the standards, then I would expect that NERC would come down and do that for us.

MR. BROWN: Yes, Alison, while I am up here, just this whole discussion is very good. I am not commenting one way or the other on how it is going, but it does indicate that there may be further developments of what folks have already seen within the SMD Proposal.

I would just urge the Commission to make sure that when there are, and if there are, significant revisions to what has already been proposed such as a mechanism for assessments, a mechanism for anything in particular that hasn't already been given to the public for its review and comment, that the Commission build into the SMD process some further mechanism to allow further public input into whatever its new proposal is. I recognize that slows things down, and I hate like heck to say that, but, nonetheless, it is probably a prudent thing to do.

MS. SILVERSTEIN: Would I be violating a confidence, Dan, to say that it is hard to imagine how SMD could be further slowed down?

MR. LARCAMP: (Laughter) No, but I am glad you said it and not me.

(Laughter.)

MS. SILVERSTEIN: That is good advice, Larry. Thank you.

Let me turn, if I may, to the issue -- oh, oh, I'm sorry. Go ahead.

We will get back to you in a second, Chuck.

MR. WEBER: Steve Weber with PriceWaterhouseCoopers. I just wanted to make a general point just to see if either FERC or NERC was aware of the New York Public Utilities Commission requirements for certification on security, and to see if there have been any linkages to make sure that there is not either redundancy? From a compliance perspective, the New York requirements require third party certification to meet those cyber-security standards.

Now, obviously that is not specific just to the energy industry, but it does capture energy, water, telecommunications and other critical infrastructure. I didn't know what types of certification or compliance linkages you were trying to make, as well as the fact that other states are trying to propose similar types of legislation.

MS. SILVERSTEIN: Roger has talked about that, hasn't he?

MR. PERRY: Yes, Roger has talked about that. Within the Advisory Group, recognizing there are 49 other states and several provinces in Canada, we are not linking our activities and our efforts to the

New York Public Utility Commission's mandates. We are cognizant of them. Personally, I view that as the higher bar. You know, there are a number of entities, PJM I believe and certainly the Midwest ISO for sure, that go through *Assess 70 Level II audit, which is just absolutely comprehensive.

You know, not only do you have to have your policies, they have got to make sense all of a sudden, and you have to demonstrate that you lock-step follow them or you get written up by auditors and it doesn't look good on your annual report. However, we haven't gone to the point of suggesting within these "low-hanging fruit" requirements that everybody run out and sign up for Assess 70 audit.

We have not suggested that everybody needs to go out and have a third party entity do a vulnerability assessment with penetration testing. Certainly, it is something that in your risk management process you need to strongly consider doing and the larger entities already do that to the largest extent, but, given that this is a widespread standard or a widespread set of requirements and the intention is the minimum daily requirements, we are at a lower level of requirements than that. I do support what you are saying; I believe it is valuable.

Just like the on-site assessment that gets done through the NERC Compliance Program, and SPP has a compliance manager, a gentleman named Ron Cecil, who does work with the external consultants that NERC uses, works with the NERC staff. We actually go out and do the on-site assessments of the SPP members and make a report back to NERC.

When SPP got evaluated earlier, just another month or so ago, NERC came down and did unto us what we have been doing to our members. A report, once again, goes back to NERC and it is reviewed by the compliance group. Like I said, if the penalties were sanctionable, then there would be penalties for areas of non-compliance that would eventually, if not initially, be financial, depending on just how badly, you know, what kind of a non-compliance issue you had.

I do believe that it is important that you periodically just check. There was a comment made, and I don't remember who the company was that made the comment about, "How can I, a senior corporate executive sitting in my ivory tower, sign off that everybody is escorted into my computer room and my control center?"

Well, technically you can't. What you can do is certify that you have a policy that says it will be done and when you go out and do a field assessment you ask somebody that should not have access into the computer room, "Hey, do you ever get into the computer room?"

And you ask somebody who does, you say, "Well, what about your visitors, do you escort your visitors, or do you just open the door and let them in?"

There are ways of ferreting out whether or not there is compliance; okay. The whole intention of this, I believe, is a reasonable attempt to comply with the requirements. I mean, I have got requirements within my shop that say if you are a visitor, if you are not someone on IT, you must be escorted into my computer room. We periodically remind the staff that this is a requirement.

That doesn't mean that 100 percent of the time some vendor or some contractor, some guy fixing the PA system has one of my staff standing around him, but it is my stated intent, and that to me is as important, if not more so, than the fact that 100 percent of the time one of my staff is babysitting the guy that is in there doing maintenance on the UPS or, like I said, fixing the PA system because it isn't working.

MS. SILVERSTEIN: Chuck, thank you for your patience.

MR. NOBLE: Okay. Thank you and thanks to

Mr. Weber I now have two points I would like to cover real quickly. I will address his first. With regards to the New York Commission, I don't disagree with what they are attempting to do. I certainly agree that it is much broader than just electric utility.

I for one would be willing to consider further discussion in how we address this around compliance assessment. If, indeed, there were such an assessment at the state level with a third party and that assessment did cover the minimum that we address, that that be taken. That would be in lieu of thus doing anything all over again and additional forms and everything else.

I think we could entertain discussion on how we could make that happen, separate from any other processes that we may have been talking about here. I think we need to do some work on that certainly with FERC and the states; okay.

The other point that I had earlier was that out of all of this we have still really been addressing the issue of compliance and assessment of compliance. The point I would like to bring out, and maybe it is a transition to another topic, is that the role I would see us playing, whether it is NERC directly or at the RTO-ISO level or within the regions themselves, wherever the assessment gets done and however we incorporate such activities by the states themselves, we are only the policemen. We are only going to issue the ticket.

They now need to come to FERC and FERC's judicial processes as to what penalties may or may not be applied. So, I think we need to make it clear that it is not the ISOs, hopefully, or the RTOs or NERC or the regions that are going to be actually slapping hands. Am I correct in that?

MS. SILVERSTEIN: A darned good question. I don't know. You know, implicit in the discussion of NERC has a compliance process and a penalty process is the notion that it would be NERC that is doing the penalizing and the issuing of whatever the fine is. The question that I was going to bring up next, the segue way for us, is in fact what about this penalty business?

Clearly, people were not happy with that FERC is swinging the ultimate hammer, which is if you are not in compliance you lose your ability to participate in the wholesale market. I can understand that. You know, so much for three strikes and you are out, this is one strike and you are out, which makes due process pretty non-trivial.

It seems to me that our first goal is not penalizing people, but fixing the problem. So, I am less interested in -- penalties get people's attention, but I want stuff fixed first period, no matter what, and after that let us worry about what the penalties are. Talk to me about that, if you would. How do we make that happen?

MR. BROWN: Alison, before we go on to that, I want to come back to the assessment. That is a very good question, but I just wanted to make sure that you folks were aware of ongoing assessment activities. There are two kinds of assessments that have been raised today.

The New York assessment, which I understand is primarily a risk assessment and then the other assessment that we were talking about just prior to that, which is a compliance assessment or a compliance audit, now I do not believe it is possible for New York to be performing a compliance audit because there isn't any standard with which to comply, so my understanding is that is simply a risk assessment.

Now, it is very clearly not a good thing, not efficient nationally to have 50 different types of risk assessments. As a result of New York's moving forward with its own concern, the Energy Assurance Office, which is currently within the Department of Energy and is going to be retitled as it is moved into the new department and broadened beyond energy assurance, is in the process of developing with another state the performance of a risk assessment which will focus, at least initially, on energy but on, more broadly also on, the critical facilities that state believes should be assessed.

Then, after that initial statewide assessment is performed, then the new department will be able to take that and create a template which, hopefully, will become a model that all states can use and then will not subject various industries to individual differing state assessments.

That is particularly of concern to some of my members who operate in many different states. That is going to go on. It is somewhat in response to the New York process, but is also just in recognition of the fact that it needs to be done. Again, that is focusing on the more basic question of risk assessment and not focusing in on the more specific question of compliance audit.

MS. SILVERSTEIN: We have a bunch of language in-house about "regional variation" and "one size does not fit all" that you could recycle very nicely and aim at OEA, if you --

MR. BROWN: Well, it is very clear that the new Department of Homeland Security is in the process of developing this, and I would encourage you and any other appropriate FERC staff as well as NERC and everybody else who is likely to be wanting to be part of that to make sure that you are part of it.

MS. SILVERSTEIN: We thought we would be restrained and let them do it without us butting in, but it happens sometimes.

Larry, did you want to say something on this?

MR. BUGH: Well, I guess within the realm of the existing NERC Compliance Program there already are, as Kevin pointed out there are, varying levels. If the program is able to actually gain the "teeth" that it really needs, there are varying levels. If I am out of compliance on a certain number of points, then certain penalties are assessed. I have to submit a report that says, "This is my plan for addressing these out of compliance issues, and this is what I am going to have them address." Then, if I fail to meet that plan to address those things, then there are other penalties assessed.

I think that the same model could be used for the cyber-security standards as well in assessing those kinds of penalties. Leave it in the hands of the FERC -- excuse me, the NERC Compliance Program. If we are going to move the thing into the NERC arena, move the whole thing into the NERC arena. Certainly, FERC may want to take a look at how those penalties are defined, how they are to be assessed, that sort of thing.

However, I believe that we could do it within the model that already exists in the NERC Compliance Program and have a pretty effective program because it then gives those folks the incentives to fix the problem, fix it as quickly as possible, and stop having to pay the penalties.

MS. SILVERSTEIN: Amen. Anybody else on the issue of penalties or compliance or verification?

MR. BROWN: On the issue of penalties, I would like to say a little something. This is just my personal opinion. This has nothing to do with EEI in particular or NERC or anybody else. Just having seen the process, it does make some sense, I believe, for FERC to operate as an appellate review board of a process that is essentially in the hands of the industry.

I think FERC within its existing jurisdiction could give penalty assessment authority to somebody, whether it is NERC or whatever it might be, but to some industry authority to assess an initial penalty while remaining the overarching review authority and the ultimate backstop, the ultimate regulator in order to maintain an oversight, and thereby obviate the need for any kind of a NAESB -- excuse me, I mean NAERO legislation, which, as has already been mentioned, no one has any idea when or if it will ever happen.

MS. SILVERSTEIN: Regardless of how that happens, how do we in the meantime while people are busy fussing about due process and negotiating penalties and that kind of stuff, how do we get the problem fixed? Is there a way to set up a provision that just says, "I say you haven't done it, and I am hiring a contractor to go in and do it to you and you are paying the bill, and we will fight about it the details later about what your penalty should have been for being non-compliant"? Or, do you have to wait to fix it until the end of the process?

MR. BROWN: Well, this perhaps reflects my bias as being a representative of the industry, and that is, I believe the industry as a whole has sufficient incentive, business incentive as well as simple patriotic incentive, to do what is necessary to be done to get the job done such that there simply isn't, certainly at this stage of the game, a need to do anything else as has been stated many times this morning.

Most of the larger players are already doing this kind of stuff anyway. I just simply don't think there is a need to address that issue at this stage, and, therefore, that gives you the time to figure out if there is a need to go that next step, to go into punishment, and how we are going to do it.

I think there is plenty of time to figure that out without having to worry today how do we do that in order to induce compliance. Because again, to repeat, I think compliance, if it is not already being done, will very shortly be done because there are darned good reasons to do it.

MS. SILVERSTEIN: I agree with that in principle, but the fact that I spend as much time as I do dealing with cranky phone calls from people and E-mails from people who don't want to have to comply with this or who oppose in principle that this should exist tells me that not everybody has done this, and my job is to get the problem fixed first and to deal with the details of what is your penalty later. I mean, yes, we all know I am results-oriented. But be warned that there will be a marker in to that effect, and you guys can clean up after I am gone.

Kevin?

MR. PERRY: Alison, almost at the risk of sounding like a broken record, I would offer once again that, as Larry pointed out earlier, the NERC compliance model, even though it is not sanctionable today by NERC, the model does exist and it is something that has been well thought out. It has been accepted by NERC membership, even though some of them may have the attitude, "Well, it don't matter because they can't do anything to me today."

It is a well-thought-out model with the graduated penalties with the requirement for identifying a mitigation plan, et cetera. I would really encourage FERC to take a strong look at that compliance model and maybe adopt it or something mighty close to it as the initial compliance for the enforceable, sanctionable compliance for these requirements until such times as it could be incorporated into another body such as NERC through their formal compliance program, clearly with the continued oversight of FERC as I assume exists today. That would be my recommendation.

I don't think we want to table this. Really, I think it does need to be part of this particular ruling. I do believe that all the players need to understand very clearly why they are incented to go and look at their policies and procedures and ensure that they have covered everything that is required, and then if they then choose not to, let the chips fall where they may, as they say.

MR. HARPER: I have a comment on the actual assessments. The electric industry is extremely large, assessments are non-trivial. The only thing I haven't heard addressed is who bears the burden for carrying out the assessments, processing the adjudication, all of that that would have to be there.

MS. SILVERSTEIN: Did you hear me ask earlier about where does NERC's money come from (laughter)?

(No verbal response.)

MS. SILVERSTEIN: Larry, where does NERC's money come from?

MR. BROWN: There is a reason why nobody has answered that question yet, and I am not going to now.

MS. SILVERSTEIN: Yet another reason I think we are looking for some legislation.

Daniel?

MR. LARCAMP: Well, it is a voluntary assessment and people pay. That is one of the things that NERC is interested in moving forward into a less voluntary a little bit more, "Yes, we can assure that your payment will show up at the end of the month in our bank account." But right now it is a voluntary assessment it is my understanding.

MS. SILVERSTEIN: I think the answer is when the NERC/NAERO problem is solved the funding mechanisms for making this happen will be much easier, or at least clearer and cleaner is I think everyone's hope. Lynn and Larry and others are nodding again.

Let me ask now, Is there anyone else in the audience who has a burning desire to say something on the topics that we have covered thus far or anything fresh that we haven't covered that you just want to -- feel the need to share?

(No verbal response.)

MS. SILVERSTEIN: No more sharing; okay.

REVIEW OF NERC'S RECOMMENDED STANDARD

MS. SILVERSTEIN: Let me ask if my Federal colleagues have any thoughts based on what you have seen in the documents before us, in the comments from parties that were filed previously, or that you have heard today? Any advice? Any cautions? Any concerns?

MR. HARPER: Well, having watched DoE grapple with the exact same issue of setting the standards across a collection of relatively independent entities, of having watched NASA, the other agencies that have similar attributes as to the power grid when setting standards, I must applaud the industry and FERC for coming together to set any minimum standards. I understand just how difficult that is.

As long as the industry is committed and they do their share and retain the professional integrity of their own assessments and do as much inside the industry as possible and leave the federal body as the final arbiter, I think you will have much greater success than taking the tact of having the external government agency get its tentacles in and regulate down to a very fine, very fine level in your process.

So, I believe the model that you are on is absolutely correct. Having watched several other processes never reach this point, I believe that this is the correct way to go.

MR. KANNBERG: For my mind, having been involved in this for a number of years, I would echo Tom's comments. The industry owns all of the infrastructure or the vast majority of it. They are the ones that are going to have to come to grips with this in their own business models in dealing with the service requirements that they have both at the federal and state level.

The issue that I think is probably foremost in my mind is the issue of compliance monitoring for self-certification. That is the one that I think is the stickiest one here and one that is going to require the greatest amount of attention. Much has been addressed relative to the potential for NERC to provide that service.

That would be wonderful, but I don't think the legislative support is there yet for that sort of role. Hopefully, it will get there soon, but then we thought that three years ago as well. So, hopefully, that shouldn't slow us from moving towards that objective.

The other concern I have is that I think it is important that we set the bar so low that compliance doesn't really provide the level of surety that we would like, and to be attentive to the fact that if we need to get a higher level of surety that we, in fact, have processes and plans that allow us to get to that point in an appropriately timely manner. Those would be the points or concerns that I might have.

MR. HALE: Frankly, that says it. I would echo that. This is an excellent first step. It does set a low bar, but it sets a bar. The cooperation that is taking place between industry association and government is certainly an example for other sectors as well, so I applaud that effort.

MS. SILVERSTEIN: Thank you.

Before I let you all get away, I need to ask you one more question and it is about our low bar. Yes, it is a low bar. But, did our friends in the industry con us? Should this bar be higher? Are there additional measures that are out there today that should be included that our industry experts dodged?

MR. HARPER: As I am sure you are well aware, that is an impossible question to give an answer with a hundred percent fidelity.

(Laughter.)

MR. HARPER: I think the process of setting a standard across the entire industry is incredibly important. Personally, yes, it is a relatively low bar. But, given the wide array of players, the resources they have available, the amount of historic legacy equipment that is out there to be dealt with, the rapidity with which technology has overtaken this industry, the non-uniformity in which this technology has been applied across the industry I am much more concerned that a bar is set and a process is in place to continually move it forward.

It is all an interconnected system. If you have a few weak spots, the entire system can fail in the IT sense, not in the NERC reliability electric power grid sense. I also believe it is very important to do it now and get that bar set because technology is going to continue to evolve faster than our ability to understand it.

Once you set the bar and you have a process, now you can begin to grapple as an industry: How do these new technologies impact us? Before we roll them in, are there things that we should do on a wider scale? So, it is a very long-winded way of saying I believe these are adequate and an appropriate first step.

MR. KANNBERG: I would agree. If I have a concern it goes back to the issue of with a low bar some maybe who already exceed this may be tempted to simply rest at their current positions, and I would hope that they would not do that. There are members of this industry that have exceeded these requirements because they feel that they have a good business reason to do so.

I would hope that the establishment of this bar would not suggest that was an imprudent investment, that, in fact, they should continue to pursue these higher levels of security. That is why I am particularly interested in seeing some intent to move to higher levels of security, and at some point in time at least to suggest that this is, in fact, not the place that we want to end up ten years from now.

MR. HALE: To build on that, I think we have to recognize that government is very slow to respond to changes, both in technology and in security risks. With that business model and the initiative and the incentive to protect their businesses, the industry is much more agile in dealing with this. It should not be, this initiative should not be, looked at as setting the standard, but rather setting a minimum bar. An industry must recognize that it is in their best business interest to protect their systems.

MR. KANNBERG: That is a good point, and it is in part why it is such a good idea for the industry to be in a prominent role in establishing the standards of performance.

MS. SILVERSTEIN: Thank you for your comments.

It has been my observation that the industry has many, many leaders who are committed to the exact kind of behavior that you all are describing and that they are well ahead of where this minimum bar is as a way to protect their own assets.

They agreed to work with us to set this low bar, again, as a way to protect their own assets from other people's failure as much as to protect the people of America and the energy systems from the failure of others, or the inability of others to be as aggressive with their resources as some companies are able to be.

I have a process suggestion for how to move forward. I think Larry's idea of we still have a few more things to work out and there has certainly been evolution of this standard over time, it sounds to me as though it may be a good idea to have a discussion with NERC on its compliance stuff.

I think this could be done constructively, and on some of the details of compliance and penalties and the adjudication sort of issues. I would like to suggest that we look at the possibility of having a joint NERC/CIPAG meeting. We would broadcast that it is going on and devote part of the agenda to these very issues, to see if we can discuss and develop these ideas further and then word smith a follow-up document that FERC could put out as a for comment.

This would be just so people know very narrowly and specifically on the cyber-security here is the new version and where it is going, and to make sure that although it has been developed by a number of people, one hopes the same players who have been active to date, that people who pay less attention to it than CIPAG members get a chance to participate and a chance to review it.

Then, we will have something that is well informed by the advance of these ideas and by additional comment as appropriate from people who have been paying attention. Maybe we can use the relationships we are developing here for you all to come back with us on testing as to how does this work, are these working, and is this a model that could be used elsewhere in other industries that we care about.

My thanks to you all for coming down on a snowy day, and you can have your afternoon back. Thank you so much.

(Whereupon, at 12:10 p.m., the Technical Conference on Cyber-Security was adjourned.)

* * * * *